REMARKS

Claims 1-16 are currently pending in the subject application, and are presently under consideration. Claims 1-16 are rejected. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

I. Objection to Claim 8

The Examiner has objected to claim 8 due to minor informalities. Claim 8 has been amended to correct the minor informalities. The amendment to claim 8 is not intended to limit claim 8 in any manner. Accordingly, Applicant's representative respectfully submits that claim 8 is no longer objectionable.

II. Rejection of Claims 1-6, 8-14 and 16 Under 35 U.S.C. §103(a)

Claims 1-6, 8-14 and 16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,192,131 to Geer, Jr. et al. ("Geer"), and further in view of U.S. Patent No. 6,615,171 to Kanevsky, et al. ("Kanevsky"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 1 recites a method for assigning certificates and associated private keys to a token, comprising accessing the token through a token reader connected to a computer system by a certificate authority and reading a token ID and a user-signature certificate from the token. Claim 1 also recites searching for a match for the token ID and the user signature certificate in an authoritative database and creating a certificate and an associated private key, wherein the certificate and the associated private key are wrapped with a public key associated with the token ID and digitally signing the certificate and the associated private key using a signature certificate of the certificate authority if a match for the token ID and the user signature certificate is found in the authoritative database. Claim 1 further recites downloading the certificate and the associated private key to the token, and decrypting the certificate and the associated private key using a private key stored in the token, such that the token stores at least the token ID, the private key, the user signature certificate and the certificate and the associated private key.

Geer taken in view of Kanevsky does not make claim 1 obvious. In rejecting claim 1, the Examiner contends that Geer discloses downloading a certificate and an associated private key to a token (See Office Action, Page 3, Citing Geer, Col. 5, Lines 15-27). Applicant's representative disagrees with this contention. The cited section of Geer discloses that an electronic merchant presents an authorization certificate to a financial institution (See Geer, Col. 4, Lines 15-18). The cited section of Geer also discloses that the financial institution verifies a signature on the authorization certificate and sends an encrypted message to the electronic merchant (See Geer, Col. 4, Lines 15-18). As stated above, claim 1 recites downloading a certificate and an associated private key to a token. Nothing in Geer teaches or suggests that the authorization certificate is downloaded to a smart card. In fact, Geer discloses that an authorization certificate is generated by a smart card (See Geer, Col. 3, Lines 24-25). Therefore, Geer taken in view of Kanevsky does not teach or suggest downloading a certificate and associated private key to a token, as recited in claim 1.

Moreover, Applicant's representative agrees that Geer does not teach or suggest searching for a token ID and a user signature certificate from a token, searching for a match for the token ID and the user signature certificate in an authoritative database and that a certificate and an associated private key are wrapped with a public key associated with the token ID if a match is found for the token ID and the user signature certificate is found in the authoritative database, as recited in claim 1. In fact, Geer is silent on a token having a token ID. Additionally, in contrast the contentions of the Examiner, the addition of Kanevsky does not make up for the deficiencies of Geer. In rejecting claim 1, the Examiner cites Col. 8, Lines 29-46 of Kanevsky. Kanevsky discloses that if a user forgets his personal identification number (PIN) that the user can reestablish his PIN by linking to an automatic speech/speaker recognition (ASSR) server 200 via a communication link to request for a PIN reset through a personal computer (PC) 450 and a smart card reader 460 (See Kanevsky, Col. 8, Lines 21-28). Kanevsky also discloses that a user provides his user ID, name and smart card serial number to the ASSR server 200 (See Kanevsky, Col. 8, Lines 31-34). Kanevsky further discloses that the ASSR server 200 accesses a stored certificate and the ASSR server 200 uses smart card's certificates and public key to encrypt a PIN reset command, which is activated by the smart card (See Col 8., Lines 35-47).

Kanevsky does not teach or suggest that a certificate and an associated private key are wrapped with a public key associated with a token ID, as recited in claim 1. Instead, Kanevsky discloses that a PIN reset command is encrypted with a smart card's certificate and public key. Clearly, the PIN reset command does not correspond to the certificate recited in claim 1. Accordingly, taken individually or in combination, Geer and Kanevsky do not teach or suggest each and every element of claim 1. Therefore, Geer taken in view of Kanevsky does not make claim 1 obvious, and claim 1 should be patentable over the cited art.

Claims 2-6 and 8 depend either directly or indirectly from claim 1, and are not obvious for at least the same reasons as claim 1, and for the specific elements recited therein. Accordingly, claims 2-6 and 8 should be patentable over the cited art.

Additionally, regarding claim 2, Geer and Kanevsky, taken individually or in combination do not teach or suggest that a certificate and an associated private key is a plurality of certificates and associated private keys, wherein at least one of the certificates and associated private keys is a signature certificate for the user, an encryption certificate and associated private key for the user, and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy, as recited in claim 2. In rejecting claim 2, the Examiner cites Col. 3, Lines 29-33 of Geer. The cited section of Geer discloses that a smart card signs an authorization certificate. Since claim 2 depends from claim 1, the certificate recited in claim 2 is downloaded to the token. Instead, as stated above, the authorization certificate disclosed in Geer is generated by the smart card. Therefore, taken individually or in combination, Geer and Kanevsky do not teach or suggest each and every element of claim 2.

Claim 9 recites a computer program embodied on a computer readable medium and executable by a computer for assigning certificates and associated private keys to a token, comprising accessing the token through a token reader connected to a computer system by a certificate authority and reading a token ID and a user signature certificate from the token.

Claim 9 also recites searching for a match for the token ID and the user signature certificate in an authoritative database and creating a certificate and an associated private key, wherein the certificate and the associated private key are wrapped with a public key associated with the token ID and digitally signing the certificate and the associated private key using a signature certificate of the certificate authority if a match for the token ID and the user signature certificate is found in the authoritative database. Claim 9 further recites downloading the certificate and the associated private key to the token, and decrypting the certificate and the associated private key using a private key stored in the token, such that the token stores at least the token ID, the private key, the user signature certificate and the certificate and the associated private key.

For the reasons state above with respect to claim 1, neither Geer nor Kanevsky, taken individually or in combination teaches or suggests downloading a certificate to a token, as recited in claim 9. Additionally, for the reasons stated above with respect to claim 1, neither Geer nor Kanevsky, taken individually or in combination, teaches or suggests a certificate and an associated private key are wrapped with a public key associated with a token ID, as recited in claim 9. Accordingly, Geer and Kanevsky, taken individually or in combination, do not teach or suggest each and every element of claim 9. Therefore, Geer taken in view of Kanevsky does not make claim 9 obvious, and claim 9 should be patentable over the cited art.

Claims 10-14 and 16 depend either directly or indirectly from claim 9, and are not obvious for at least the same reasons as claim 9 and for the specific elements recited therein. Accordingly, claims 10-14 and 16 should be patentable over the cited art.

Additionally, regarding claim 10, claim 10 is similar to claim 2, and is not made obvious by Geer taken in view of Kanevsky for substantially the same reasons as stated above with respect to claim 2. That is, neither Geer nor Kanevsky, taken individually or in combination, teaches or suggests that a certificate and an associated private key is a plurality of certificates and associated private keys, wherein at least one of the certificates and associated private keys is a signature certificate for the user, an encryption certificate and associated private key for the user, and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy, as recited in claim 10. Accordingly, Geer and Kanevsky, taken individually or in combination, fail to teach or suggest each and every element of claim 10.

For the reasons described above, claims 1-6, 8-14 and 16 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

III. Rejection of Claims 7 and 15 Under 35 U.S.C. §103(a)

Claims 7 and 15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Geer and Kanevsky, and further in view of U.S. Publication No. 2003/0005291 to Burn ("Burn"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 7 and 15 depend from claims 1 and 9, respectively and are not obvious for at least the same reasons as claims 1 and 9. The further addition of Burn does not make up for the aforementioned deficiencies of Geer taken in view of Kanevsky.

Additionally, Applicant's representative agrees that Geer taken in view of Kanevsky does not teach or suggest decrypting a certificate and associated private key using a private key stored in the token requires the entry of a passphrase by a user, as recited in claims 7 and 15. Applicant's representative respectfully submits that Geer, Kanevsky and Burn teach away from their respective combination and modification in the manner suggested by the Examiner. The U.S. Court Appeals for the Federal Circuit has held that references teach away from combination if the references taken in combination would produce a seemingly inoperable device. *McGinley v. Franklin Sports Inc.*, 262 F.3d 1339, 1354, 60 U.S.P.Q.2d 1001, 1010 (Fed. Cir. 2001). In Kanevsky, the only reason taught or suggested for sending a PIN reset command, as discussed above with respect to claim 1, is when a user forgets his/her PIN. Accordingly, a user in such a situation would not be able to enter a PIN. In contrast, claims 7 and 15 require that a passphrase be entered by a user. If the teachings of Geer and Kanevsky were combined and modified with Burn such that a user were required to enter a PIN when the user forgot his/her PIN, the user would not be able to decrypt the PIN reset command, since that user would not be able to remember his/her PIN. Accordingly, Applicant's representative respectfully submits that combining and modifying the teachings of Geer, Kanevsky and Burn in the manner suggested by the Examiner would result in an inoperable device, and thus, the references teach away from their combination.

For the reasons described above, claims 7 and 15 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

In view of the foregoing remarks, Applicant's representative respectfully submits that the present application is in condition for allowance. Applicant's representative respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 7-11-06

Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
1300 EAST NINTH STREET, SUITE 1700
CLEVELAND, OHIO 44114
Phone: (216) 621-2234
Fax: (216) 621-4072